and mouse 220 all connected via a common bus 222. In operation the central processing unit 202 will execute computer program instructions that may be stored in one or more of the random access memory 204, the read only memory 206 and the hard disk drive 210 or dynamically downloaded via the network interface card 208. The results of the processing performed may be displayed to a user via the display driver 212 and the monitor 214. User inputs for controlling the operation of the general purpose computer 200 may be received via the user input output circuit 216 from the keyboard 218 or the mouse 220. It will be appreciated that the computer program could be written in a variety of different computer languages. The computer program may be stored and distributed on a recording medium or dynamically downloaded to the general purpose computer 200. When operating under control of an appropriate computer program, the general purpose computer 200 can perform the above described techniques and can be considered to form an apparatus for performing the above described technique. The architecture of the general purpose computer 200 could vary considerably and Figure 6 is only one example.

Although illustrative embodiments of the invention have been described in detail herein with reference to the accompanying drawings, it is to be understood that the invention is not limited to those precise embodiments, and that various changes and modifications can be effected therein by one skilled in the art without departing from the scope and spirit of the invention as defined by the appended claims.

WE CLAIM:

1. A computer program product for controlling a computer, said computer program product comprising:

malware infection detecting logic operable to detect a malware infection of at least one computer; and

device disabling logic operable upon detection of said malware infection to disable operation of one or more data I/O devices of said at least one computer.

2. A computer program product as claimed in claim 1, wherein said malware infection detection logic detects a malware infection by one or more of:

positively identifying an item of malware upon said at least one computer; and

identifying behaviour of said at least one computer indicative of malware infection.

3. A computer program product as claimed in claim 1, wherein said one or more data I/O devices include one or more of:

a floppy disk drive;

a compact disk drive;

a removable media drive; and

a network interface card.

4. A computer program product as claimed in claim 1, wherein said device disabling logic is operable upon detection of malware infection to disable at least one data I/O device of at least one further computer.

5. A computer program product as claimed in claim 1, wherein said device disabling logic is operable to require user confirmation prior to disabling said one or more data I/O devices.

6. A computer program product as claimed in claim 1, wherein said device disabling logic is operable to disable said one or more data I/O devices using an API call to an operating system of said at least one computer.

7. A computer program product for controlling a computer, said computer program product comprising:

device disabling logic operable upon receipt by a computer of a command indicative of malware infection precautions being taken to disable operation of one or more data I/O devices of said computer.

8. A computer program product as claimed in claim 7, wherein said one or more data I/O devices include one or more of:

a floppy disk drive;

a compact disk drive;

a removable media drive; and

a network interface card.

9. A computer program product as claimed in claim 7, wherein said device disabling logic is operable to disable said one or more data I/O devices using an API call to an operating system of said at least one computer.

10. A computer program product for controlling a computer, said computer program product comprising:

user input logic operable to receive a user input indicative of activating precautions against a malware infection; and

device disabling logic operable upon receipt of said user input to disable operation of one or more data I/O devices of said at least one computer.

11. A computer program product as claimed in claim 10, wherein said one or more data I/O devices include one or more of:

a floppy disk drive;

a compact disk drive;

a removable media drive; and

a network interface card.

12. A computer program product as claimed in claim 10, wherein said device disabling logic is operable upon detection of malware infection to disable at least one data I/O device of at least one further computer.

13. A computer program product as claimed in claim 10, wherein said device disabling logic is operable to disable said one or more data I/O devices using an API call to an operating system of said at least one computer.

14. A method of protecting against malware infection, said method comprising the steps of:

detecting a malware infection of at least one computer; and

upon detection of said malware infection disabling operation of one or more data I/O devices of said at least one computer.

15. A method as claimed in claim 14, wherein detection of a malware infection is by one or more of:

positively identifying an item of malware upon said at least one computer; and

identifying behaviour of said at least one computer indicative of malware infection.

16. A method as claimed in claim 14, wherein said one or more data I/O devices include one or more of:

a floppy disk drive;

a compact disk drive;

a removable media drive; and

a network interface card.

17. A method as claimed in claim 14, wherein upon detection of malware infection at least one data I/O device of at least one further computer is disabled.

18. A method as claimed in claim 14, wherein user confirmation is required prior to disabling said one or more data I/O devices.

19. A method as claimed in claim 14, wherein disabling said one or more data I/O devices uses an API call to an operating system of said at least one computer.

20. A method of protecting against malware infection, said method comprising the steps of:

upon receipt by a computer of a command indicative of malware infection precautions being taken disabling operation of one or more data I/O devices of said computer.

21. A method as claimed in claim 20, wherein said one or more data I/O devices include one or more of:

a floppy disk drive;

a compact disk drive;

a removable media drive; and

a network interface card.

22. A method as claimed in claim 20, wherein disabling said one or more data I/O devices uses an API call to an operating system of said at least one computer.

23. A method of protecting against malware infection, said method comprising the steps of:

receiving a user input indicative of activating precautions against a malware infection; and

upon receipt of said user input disabling operation of one or more data I/O devices of said at least one computer.

24. A method as claimed in claim 23, wherein said one or more data I/O devices include one or more of:

a floppy disk drive;

a compact disk drive;

a removable media drive; and

a network interface card.

25. A method as claimed in claim 23, wherein upon detection of malware infection disabling at least one data I/O device of at least one further computer.

26. A method as claimed in claim 23, wherein disabling said one or more data I/O devices uses an API call to an operating system of said at least one computer.

27. Apparatus for protecting against malware infection, said apparatus comprising:

a malware infection detector operable to detect a malware infection of at least one computer; and

a device disabling unit operable upon detection of said malware infection to disable operation of one or more data I/O devices of said at least one computer.

28. Apparatus as claimed in claim 27, wherein said malware infection detector detects a malware infection by one or more of:

positively identifying an item of malware upon said at least one computer; and

identifying behaviour of said at least one computer indicative of malware infection.

29. Apparatus as claimed in claim 27, wherein said one or more data I/O devices include one or more of:

a floppy disk drive;

a compact disk drive;

a removable media drive; and

a network interface card.

30. Apparatus as claimed in claim 27, wherein said device disabling unit is operable upon detection of malware infection to disable at least one data I/O device of at least one further computer.

31. Apparatus as claimed in claim 27, wherein said device disabling unit is operable to require user confirmation prior to disabling said one or more data I/O devices.

32. Apparatus as claimed in claim 27, wherein said device disabling unit is operable to disable said one or more data I/O devices using an API call to an operating system of said at least one computer.

33. Apparatus for protecting against malware infection, said apparatus comprising:

a device disabling unit operable upon receipt by a computer of a command indicative of malware infection precautions being taken to disable operation of one or more data I/O devices of said computer.

34. Apparatus as claimed in claim 33, wherein said one or more data I/O devices include one or more of:

a floppy disk drive;

a compact disk drive;

a removable media drive; and

a network interface card.

35. Apparatus as claimed in claim 33, wherein said device disabling unit is operable to disable said one or more data I/O devices using an API call to an operating system of said at least one computer.

36. Apparatus for protecting against malware infection, said apparatus comprising:

a user input unit operable to receive a user input indicative of activating precautions against a malware infection; and

a device disabling unit operable upon receipt of said user input to disable operation of one or more data I/O devices of said at least one computer.

37. Apparatus as claimed in claim 36, wherein said one or more data I/O devices include one or more of:

a floppy disk drive;

a compact disk drive;

a removable media drive; and

a network interface card.

38. Apparatus as claimed in claim 36, wherein said device disabling unit is operable upon detection of malware infection to disable at least one data I/O device of at least one further computer.

39. Apparatus as claimed in claim 36, wherein said device disabling unit is operable to disable said one or more data I/O devices using an API call to an operating system of said at least one computer.